NAT およびファイアウォールの SIP ALG の強化

NAT およびファイアウォールの SIP ALG の強化機能は、ネットワーク アドレス変換（NAT）およびファイアウォールの既存の Session Initiation Protocol（SIP）アプリケーション レベル ゲートウェイ（ALG）サポートを介してより適切なメモリ管理と RFC 準拠を提供します。 この機能は、次の拡張機能を提供します。

- すべての SIP レイヤ 7 データのローカル データベースの管理
- Via ヘッダーの処理
- 追加の SIP メソッドのロギングのサポート
- Provisional Response ACKnowledgment（PRACK）コール フローのサポート
- Record-Route ヘッダーのサポート

上記の拡張機能は、デフォルトで利用可能です。NAT またはファイアウォールに対する追加の設定は必要ありません。

このモジュールでは、SIP ALG 拡張機能について説明し、SIP 用の NAT およびファイアウォール サポートを有効にする方法について説明します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の注意事項と機能情報については、Bug Search Tool およびご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

NAT およびファイアウォールの SIP ALG の強化の制約事項

- Session Initiation Protocol（SIP）アプリケーション レベル ゲートウェイ（ALG）は、セキュリティ機能を提供しません。
- SIP ALG は、コール ID に基づいてローカル データベースを管理します。 2 つのコールが同じコール ID で 2 つの異なるクライアントから発信され、結果としてコール ID が重複するというまれで厄介なケースが発生する場合があります。

NAT およびファイアウォールの SIP ALG の強化について

SIP の概要

Session Initiation Protocol（SIP）は、1 人または複数の参加者とのセッションを作成、変更、および終了するためのアプリケーション層コントロール（シグナリング）プロトコルです。 SIP セッションには、インターネット電話の通話、マルチメディアの配布、マルチメディア会議などがあります。 SIP は HTTP のような要求/応答トランザクション モデルに基づいています。 各トランザクションは、サーバで特定のメソッドまたは関数を呼び出す 1 つの要求と 1 つ以上の応答で構成されます。

セッションの作成に使用される SIP の招待は、互換性のあるメディア タイプのセットに参加者が同意できるセッション記述を伝送しています。 SIP は、プロキシ サーバと呼ばれる要素を利用して、ユーザの所在地への要求のルーティング、サービスのためのユーザ認証および認可、プロバイダーのコールルーティング ポリシーの実装、およびユーザへの機能提供を行っています。 また、SIP には、プロキシ サーバから使用できるように、ユーザの所在地をアップロードできる登録機能があります。 SIP は複数のトランスポート プロトコルを基礎として実行されます。

アプリケーション レベル ゲートウェイ

アプリケーション レベル ゲートウェイ（ALG）は、アプリケーション層ゲートウェイとも呼ばれ、アプリケーションパケットのペイロード内のIPアドレス情報を変換するアプリケーションです。 ALG は、アプリケーション層プロトコルを解釈し、ファイアウォールおよびネットワーク アドレス変換（NAT）アクションを実行するために使用されます。 これらのアクションは、ファイアウォールおよび NAT の設定に応じて次の 1 つまたは複数のアクションになります。

- クライアント アプリケーションが、ダイナミック TCP または UDP ポートを使用してサーバ アプリケーションと通信できるようにします。
- アプリケーション固有のコマンドを認識し、それらに対するきめ細かいセキュリティ制御を提供します。
- データ交換を行う 2 台のホスト間のデータの複数のストリームまたはセッションを同期します。
- アプリケーション ペイロードで使用できるネットワーク層アドレス情報を変換します。

ファイアウォールはピンホールを開き、NATは、アプリケーション層データ ストリームの送信元および宛先 IP アドレスを伝送しない TCP または UDP トラフィックに対する変換サービスを実行します。 IPアドレス情報を埋め込む特定のプロトコルまたはアプリケーションにはALGのサポートが必要です。

SIP ALG ローカル データベース管理

Session Initiation Protocol（SIP）トランクは、SIP を使用した IP ネットワーク上のサービス プロバイダーへの IP PBX の直接接続です。 SIP トランクには多数の同時コールが存在する可能性があります。 コール設定プロセス中、すべてのコールが、コールの確立に同じ制御チャネルを使用します。 複数のコールが、コール設定に同じ制御チャネルを使用します。 同じ制御チャネルが複数のコールで使用されると、制御チャネル セッションに保存されたステートフル情報は、信頼できないものになります。 SIP ステートフル情報は、メディア データを送信するためにクライアントおよびサーバ エンドポイントが使用する IP アドレスやポート番号などのメディア チャネル情報で構成されます。 メディア チャネル情報を使用して、ファイアウォール ピンホールおよびネットワーク アドレス変換（NAT）ドアが、ファイアウォールおよび NAT のデータ チャネルにそれぞれ作成されます。 複数のコールがコース設定に同じ制御チャネルを使用するため、複数のメディア データ セットが存在することになります。

SIP トランクで、複数のコールが、同じファイアウォールおよび NAT セッションを共有します。 NAT およびファイアウォールは、SIP パケットの 5 タプル（送信元アドレス、宛先アドレス、送信元ポート、宛先ポート、およびプロトコル）を使用して SIP セッションを識別および管理します。 コールの識別および照合に 5 タプルを使用する従来の方式は、SIP トランキングを完全にサポートしているわけではなく、多くの場合、レイヤ 7 データ メモリ リークやコール照合の問題を招きます。

他のアプリケーション レベル ゲートウェイ（ALG）とは対照的に、SIP ALG は、ローカル データベースを使用して通常の SIP コールおよび SIP トランクに埋め込まれた SIP コールに含まれる

すべてのメディア関連情報を保存することで、SIP レイヤ 7 データを管理します。 SIP ALG は、SIP メッセージに含まれる Call-ID ヘッダー フィールドを使用して、コール照合に関してローカル データベースを検索し、コールを管理および終了します。 Call-ID ヘッダー フィールドは、同じ SIP ダイアログに属するメッセージを識別するダイアログ識別子です。

SIP ALG は、コール ID を使用して、ローカル データベースで検索を実行し、メモリ リソースを管理します。 SIP ALG がレイヤ 7 データ レコードをデータベースから解放できない特定のシナリオでは、セッション タイマーを使用してリソースの管理および解放が行われ、データベース内に停止状態のコール レコードが残らないようにします。

（注） すべてのレイヤ 7 データは、ローカル データベースを使用して SIP ALG によって管理されるため、SIP ALG は、SIP レイヤ 7 データの解放をファイアウォールおよび NAT には依存せず、自分でデータを解放します。 **clear** コマンドを使用して、すべての NAT 変換およびファイアウォール セッションをクリアしている場合、ローカル データベース内の SIP レイヤ 7 データは解放されません。

SIP ALG Via ヘッダー サポート

Session Initiation Protocol（SIP）INVITE 要求には、Via ヘッダー フィールドが含まれます。 Via ヘッダー フィールドは、SIP 要求が通過する転送パスを示します。 Via ヘッダーには、後続の SIP 応答のリターン パスに関する情報も含まれます。これには、応答メッセージが送信される IP アドレスおよびポートが含まれます。

SIP ALG では、確認応答（ACK）メッセージを除き、受信した各 SIP 要求の Via ヘッダー フィールドの最初の値に基づいてファイアウォール ピンホールまたはネットワーク アドレス変換（NAT）ドアを作成します。 ポート番号情報が、最初の Via ヘッダーで欠落している場合、ポート番号は 5060 と見なされます。

SIP ALG メソッド ロギングのサポート

NAT およびファイアウォールの SIP ALG の強化機能は、Session Initiation Protocol（SIP）アプリケーション レベル ゲートウェイ（ALG）統計情報の次のメソッドの詳細なロギングをサポートします。

- PUBLISH
- OPTIONS
- 1XX（100、180、183 を除く）
- 2XX（200 を除く）

SIP ALG 統計情報に記録された既存の SIP メソッドには、ACK、BYE、CANCEL、INFO、INVITE、MESSAGE、NOTIFY、REFER、REGISTER、SUBSCRIBE、および 1XX-6XX が含まれます。

SIP ALG PRACK コール フローのサポート

Session Initiation Protocol（SIP）では、最終応答と暫定応答の 2 種類の応答が定義されています。最終応答は、要求の処理結果を伝え、信頼性のある方法で送信されます。 一方、暫定応答は、要求処理の進捗状況に関する情報を提供しますが、信頼性のある方法では送信されません。

Provisional Response ACKnowledgment（PRACK）は、確認応答（ACK）システムを暫定応答に提供する SIP メソッドです。 PRACK を使用すると、SIP エンドポイント間の SIP の暫定応答を確実に交換できます。 SIP の信頼性の高い暫定応答によってメディア情報の交換が保証され、コールの接続前にリソース予約を実行できます。

SIP は、接続ネゴシエーション中、セッション記述プロトコル（SDP）の接続、メディア、および属性のフィールドを使用します。 SIP アプリケーション レベル ゲートウェイ（ALG）は、PRACK メッセージ内の SDP 情報をサポートします。 メディア情報が PRACK メッセージに存在する場合、SIP ALG はメディア情報を取得して処理します。 SIP ALG は、以降のメディア ストリームのメディア チャネルの作成も処理します。 SIP ALG は、PRACK メッセージの SDP 情報に基づいて、ファイアウォール ピンホールおよび NAT ドアを作成します。

SIP ALG Record-Route ヘッダー サポート

Record-Route ヘッダー フィールドは、SIP ダイアログの今後の要求がプロキシ経由でルーティングされるよう強制するために、Session Initiation Protocol（SIP）プロキシによって SIP 要求に追加されました。 これで、ダイアログ内で送信されるメッセージはすべての SIP プロキシを通過し、これにより、Record-Route ヘッダー フィールドが SIP 要求に追加されます。 Record-Route ヘッダー フィールドには、プロキシを識別する、グローバルに到達可能な Uniform Resource Identifier（URI）が含まれます。

SIP アプリケーション レベル ゲートウェイ（ALG）は、Contact ヘッダーを解析し、Contact ヘッダーの IP アドレスとポートの値を使用して、ファイアウォール ピンホールおよびネットワーク アドレス変換（NAT）ドアを作成します。 さらに、SIP ALG は、プロキシ経由でルーティングされる今後のメッセージ用のファイアウォール ピンホールおよび NAT ドアを作成するための Record-Route ヘッダーの解析をサポートします。

Record-Route ヘッダーの解析では、SIP ALG は次のシナリオをサポートします。

- Cisco ASR 1000 アグリゲーション サービス ルータが、2 つのプロキシの間に配置されます。
- Cisco ASR 1000 アグリゲーション サービス ルータが、ユーザ エージェント クライアント（UAC）とプロキシの間に配置されます。
- Cisco ASR 1000 アグリゲーション サービス ルータが、プロキシとユーザ エージェント サーバ（UAS）の間に配置されます。
- クライアントとサーバ間にプロキシは存在しません。 このシナリオではレコード ルーティングは発生しません。

NAT およびファイアウォールの SIP ALG の強化の設定方法

SIP の NAT サポートのイネーブル化

SIP の NAT サポートは、ポート 5060 でデフォルトでイネーブルになっています。この機能がディセーブルになっている場合、SIP の NAT サポートを再びイネーブルにするには、この作業を実行します。SIP の NAT サポートをディセーブルにするには、**no ip nat service sip** コマンドを使用します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip nat service sip** {**tcp** | **udp**} **port** *port-number*
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip nat service sip** {**tcp** | **udp**} **port** *port-number* 例： `Device(config)# ip nat service sip tcp port 5060`	SIP の NAT サポートをイネーブルにします。
ステップ 4	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

SIP インスペクションのイネーブル化

手順の概要

1. **enable**
2. **configure terminal**
3. **class-map type inspect match-any** *class-map-name*
4. **match protocol** *protocol-name*
5. **exit**
6. **policy-map type inspect** *policy-map-name*
7. **class type inspect** *class-map-name*
8. **inspect**
9. **exit**
10. **class class-default**
11. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**class-map type inspect match-any** *class-map-name* 例： `Device(config)# class-map type inspect match-any sip-class1`	検査タイプ クラス マップを作成し、クラス マップ コンフィギュレーション モードを開始します。
ステップ 4	**match protocol** *protocol-name* 例： `Device(config-cmap)# match protocol sip`	指定されたプロトコルに基づいてクラス マップの一致基準を設定します。

	コマンドまたはアクション	目的
ステップ 5	**exit** 例： `Device(config-cmap)# exit`	クラスマップ コンフィギュレーション モードを終了します。
ステップ 6	**policy-map type inspect** *policy-map-name* 例： `Device(config)# policy-map type inspect sip-policy`	検査タイプ ポリシー マップを作成し、ポリシー マップ コンフィギュレーション モードを開始します。
ステップ 7	**class type inspect** *class-map-name* 例： `Device(config-pmap)# class type inspect sip-class1`	アクションを実行するクラスを指定し、ポリシーマップ クラス コンフィギュレーション モードを開始します。
ステップ 8	**inspect** 例： `Device(config-pmap-c)# inspect`	ステートフル パケット インスペクションをイネーブルにします。
ステップ 9	**exit** 例： `Device(config-pmap-c)# exit`	ポリシー マップ クラス コンフィギュレーション モードを終了し、ポリシーマップ コンフィギュレーションモードに戻ります。
ステップ 10	**class class-default** 例： `Device(config-pmap)# class class-default`	これらのポリシー マップ設定が事前に定義したデフォルト クラスに適用されることを指定します。 • 設定済みクラス マップの一致基準のいずれともトラフィックが一致しない場合、事前に定義されたデフォルト クラスに誘導されます。
ステップ 11	**end** 例： `Device(config-pmap)# end`	ポリシーマップ クラス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

ゾーン ペアの設定および SIP ポリシー マップの付加

手順の概要

1. **enable**
2. **configure terminal**
3. **zone security** {*zone-name* | **default**}
4. **exit**
5. **zone security** {*zone-name* | **default**}
6. **exit**
7. **zone-pair security** *zone-pair-name* [**source** {*source-zone-name* | **self** | **default**} **destination** [*destination-zone-name* | **self** | **default**]]
8. **service-policy type inspect** *policy-map-name*
9. **exit**
10. **interface** *type number*
11. **zone-member security** *zone-name*
12. **exit**
13. **interface** *type number*
14. **zone-member security** *zone-name*
15. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**zone security** {*zone-name*	**default**} 例： `Device(config)# zone security zone1`	インターフェイスを割り当てることができるセキュリティ ゾーンを作成し、セキュリティ ゾーン コンフィギュレーション モードを開始します。
ステップ 4	**exit** 例： `Device(config-sec-zone)# exit`	セキュリティ ゾーン コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。

	コマンドまたはアクション	目的
ステップ 5	**zone security** {*zone-name* | **default**} 例： `Device(config)# zone security zone2`	インターフェイスを割り当てることができるセキュリティ ゾーンを作成し、セキュリティ ゾーン コンフィギュレーション モードを開始します。
ステップ 6	**exit** 例： `Device(config-sec-zone)# exit`	セキュリティ ゾーン コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 7	**zone-pair security** *zone-pair-name* [**source** {*source-zone-name* | **self** | **default**} **destination** [*destination-zone-name* | **self** | **default**]] 例： `Device(config)# zone-pair security in-out source zone1 destination zone2`	ゾーン ペアを作成し、セキュリティ ゾーンペア コンフィギュレーション モードに戻ります。 （注） ポリシーを適用するには、ゾーン ペアを設定する必要があります。
ステップ 8	**service-policy type inspect** *policy-map-name* 例： `Device(config-sec-zone-pair)# service-policy type inspect sip-policy`	ファイアウォール ポリシー マップを宛先ゾーン ペアに付加します。 （注） ゾーンのペア間でポリシーが設定されない場合、トラフィックはデフォルトでドロップされます。
ステップ 9	**exit** 例： `Device(config-sec-zone-pair)# exit`	セキュリティ ゾーンペア コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 10	**interface** *type number* 例： `Device(config)# interface gigabitethernet 0/0/0`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 11	**zone-member security** *zone-name* 例： `Device(config-if)# zone-member security zone1`	インターフェイスを指定したセキュリティ ゾーンに割り当てます。

	コマンドまたはアクション	目的
		（注） インターフェイスをセキュリティゾーンのメンバーにした場合、方向に関係なくインターフェイスを通過するすべてのトラフィック（デバイス宛のトラフィックまたはデバイス発信のトラフィックを除く）は、デフォルトでドロップされます。 トラフィックがインターフェイス通過するには、ゾーンをポリシーの適用先のゾーン ペアの一部にする必要があります。 ポリシーがトラフィックを許可すると、トラフィックはそのインターフェイスを通過できます。
ステップ 12	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 13	**interface** *type number* 例： `Device(config)# interface gigabitethernet 0/1/1`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 14	**zone-member security** *zone-name* 例： `Device(config-if)# zone-member security zone2`	インターフェイスを指定したセキュリティ ゾーンに割り当てます。
ステップ 15	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

NAT およびファイアウォールの SIP ALG の強化の設定例

例：SIP の NAT サポートのイネーブル化

```
Device> enable
Device# configure terminal
Device(config)# ip nat service sip tcp port 5060
Device(config)# end
```

例：SIP インスペクションのイネーブル化

```
class-map type inspect match-any sip-class1
 match protocol sip
!
policy-map type inspect sip-policy
 class type inspect sip-class1
  inspect
!
class class-default
```

例：ゾーン ペアの設定および SIP ポリシー マップの付加

```
zone security zone1
!
zone security zone2
!
zone-pair security in-out source zone1 destination zone2
 service-policy type inspect sip-policy
!
interface gigabitethernet 0/0/0
 zone security zone1
!
interface gigabitethernet 0/1/1
 zone security zone2
```

NAT およびファイアウォールの SIP ALG の強化の追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
NAT 設定	『*IP Addressing: NAT Configuration Guide*』
ファイアウォールの設定	『*Security Configuration Guide: Zone-Based Policy Firewall*』
NAT コマンド	『Cisco IOS IP Addressing Services Command Reference』
ファイアウォール コマンド	• 『Cisco IOS Security Command Reference: Commands A to C』 • 『Cisco IOS Security Command Reference: Commands D to L』 • 『Cisco IOS Security Command Reference: Commands M to R』 • 『Cisco IOS Security Command Reference: Commands S to Z』

関連項目	マニュアル タイトル
NAT とファイアウォールの ALG のサポート	『NAT and Firewall ALG and AIC Support on Cisco ASR 1000 Series Aggregation Services Routers』マトリクス

標準および RFC

標準/RFC	タイトル
RFC 3261	『*SIP: Session Initiation Protocol*』

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

NAT およびファイアウォールの SIP ALG の強化の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。 この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。 その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

表 *1*：*NAT* およびファイアウォールの *SIP ALG* の強化の機能情報

機能名	リリース	機能情報
NAT およびファイアウォールの SIP ALG の強化	Cisco IOS XE Release 3.8S	NAT およびファイアウォールの SIP ALG の強化機能は、NAT およびファイアウォールの既存の SIP ALG サポートを介してより適切なメモリ管理と RFC 準拠を提供します。